УГОЛОВНЫЙ ПРОЦЕСС. КРИМИНАЛИСТИКА. ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

УДК 343.98

К ВОПРОСУ О КЛАССИФИКАЦИИ ЦИФРОВЫХ СЛЕДОВ

А. С. Апекунов
преподаватель кафедры оперативно-розыскной деятельности
факультета милиции Могилевского института МВД (Беларусь)

А. С. Варванович
участковый инспектор милиции ООПП МОБ ОВД
Наровлянского районного исполнительного комитета,
магистрант Академии МВД Республики Беларусь

В статье рассмотрены теоретические подходы к построению классификации цифровых следов в криминалистике. Установлено, что в настоящее время в криминалистической науке отсутствует единообразный подход к определению сущности цифровых следов. На основе анализа существующих научных взглядов на обозначенную проблему предложена авторская классификация, определена сущность цифровых следов с точки зрения природы их возникновения и существования.

Ключевые слова: *электронный след, виртуальный след, информационный след, электронно-цифровой след, цифровой след, киберпреступность.*

В криминалистической науке классификационный подход при установлении имеющихся связей между объектами единой природы происхождения на основе анализа их сущности и свойств применяется достаточно широко. Опираясь на диалектические принципы, классификации переносят центр внимания на раскрытие внутренних закономерных связей между группами классифицируемых предметов, отражают момент их зарождения и изменения, логические связи и отношения между ними, при этом они должны обладать максимальной гибкостью и исключать искусственность, произвольность и субъективизм [1, с. 523].

В теоретических источниках, посвященных исследованию цифровых следов, отсутствует четкая система устоявшихся оснований классификации, в то же время с точки зрения криминалистической науки они имеют существенное значение, в частности, при определении источника доказательственной информации, например, в связи с установлением способа совершения преступления, личности преступника. Кроме того, на определенном этапе они могут иметь самостоятельное значение, например, при определении общности их происхождения и последующей идентификации.

Согласно правилам формальной логики, основания классификации должны занимать в ней строго определенное место и быть рассчитаны на долговременное использование без каких-либо существенных изменений. Таким образом, основная задача классификации состоит в том, чтобы систематизировать область знаний для обеспечения ориентации как в научной, так и практической деятельности [2, с. 177]. Р. С. Белкин отмечал: «В криминалистической науке мы имеем дело с логическими классификациями, в практике борьбы с преступностью — с предметными классификациями, точнее — с предметным классифицированием на основе научной, или эмпирической, классификации. <…> Частные криминалистические классификации есть существенная часть криминалистической систематики. Помимо своего гносеологического значения как одного из средств познания, эти классификации представляют собой и одно из средств практической деятельности, разрабатываемое криминалистикой специально для борьбы с преступностью» [3, с. 130, 133].

В юридической литературе, посвященной исследованию цифровых следов, приводятся различные классификации как по структуре, так и по используемым основаниям. А. Л. Осипенко предлагает использовать классификацию по способу создания цифровых данных в виде файлов:

1. Файлы, созданные пользователем и сохраненные на материальном носителе устройства.
2. Файлы, созданные в автоматическом режиме без участия пользователя.
3. Файлы, в которых записи могут быть сгенерированы устройством с учетом управляющих последовательностей, определенных пользователем [4].

Исследователь А. Н. Колычева предлагает авторскую классификацию электронно-цифровых следов, образующихся в процессе подготовки, совершения и сокрытия преступного деяния, образующихся в компьютерной системе и интернет-пространстве, по виду информации [5, с. 37–40]:

1. Файлы системного и прикладного программного обеспечения.
2. Файлы конфигурации программных приложений и операционных систем.
3. Файлы-журналы программного обеспечения и технических средств.
4. Файлы — источники информации, образующиеся в ходе деятельности пользователя, в том числе их резервные копии и удаленные файлы, подлежащие восстановлению.
5. Файлы, обеспечивающие аутентификацию и конфиденциальность пользователей.
6. Информация, находящаяся в оперативной памяти или файле подкачки устройства.
7. Информация, полученная с помощью соответствующих радиоэлектронных или специальных технических средств.

Используя в качестве основания классификации цифровых следов по их местонахождению, автор выделяет следующие их группы:

1. Находящиеся на электронных устройствах потерпевшего.
2. Находящиеся на электронных устройствах лиц, подготавливающих, совершающих либо совершивших преступление.
3. Находящиеся на материальных носителях, размещенных в технических устройствах операторов электросвязи [5, с. 40].

По источнику хранения цифровые следы классифицируются на:

1. Следы на материальных носителях.
2. Следы, находящиеся в оперативной памяти электронных устройств получения, фиксации, обработки и передачи цифровых данных.
3. Следы в сетевых каналах передачи данных между устройствами [5, с. 40].

Некоторые авторы, опираясь на специфику подготовки, совершения и сокрытия отдельных видов преступлений, обоснованно полагают, что цифровые следы могут быть классифицированы и более подробно. В частности, применительно к совершению мошенничества с помощью средств сотовой связи предлагается следующая классификация:

1. Цифровые следы, возникающие в мобильных средствах телекоммуникации (голосовые сообщения в виде акустических сигналов, СМС-сообщения и др.):

– сведения об используемом оконечном оборудовании, номерах терминалов, об абонентах сети;

– пространственно-временные данные (расположение базовых станций, время, период и продолжительность соединений);

– метаданные контактов, фотографий, аудио- и видеозаписей;

– наличие программ записи акустических сигналов и их изменения, специальные программные приложения для проведения банковских операций.

2. Цифровые следы, связанные с использованием банковской карты (банковского счета).

3. Аудиофонограммы.

4. Цифровые следы, связанные с подготовкой, совершением и сокрытием преступного деяния, находящиеся на электронном устройстве преступника [6].

В работе А. Г. Себякина на основании проведенного анализа предлагается классификация цифровых следов по степени воздействия пользователя на компьютерную систему. По мнению автора классификации, такие следы делятся на непосредственные и опосредованные. Под непосредственными следами в указанном случае следует понимать электронно-цифровые следы, возникающие в результате непосредственного воздействия пользователя на компьютерную систему. Указанные следы могут находиться как непосредственно на материальном носителе электронного устройства, так и вне его (доступ к которым обеспечивается с применением средств телекоммуникации, т. е. канала связи). Под опосредованными следами автор понимает цифровые следы, образованные в результате функционирования системного программного обеспечения, стандартами форматов файлов и протоколов передачи данных вне зависимости от воли пользователя [7, с. 49].

Исходя из изложенного, согласимся с мнением автора о том, что предложенная им классификация имеет не только теоретическую сторону, она содержит и практический аспект, поскольку принадлежность цифрового следа к непосредственным или опосредованным может определять уровень применения специальных знаний и криминалистической техники, необходимых для его обнаружения.

Заслуживает внимания классификация цифровых следов, изложенная в работе А. А. Жижилевой, в которой автор дифференцирует цифровые следы на два основных вида — активные и пассивные:

1. Активный цифровой след — сознательная деятельность субъекта в информационно-телекоммуникационном пространстве (переписка, ведение блогов, комментарии).

2. Пассивный виртуальный след — совокупность данных, оставленных пользователем непреднамеренно (история посещения сайтов, IP-адрес и т. д.) [8].

Данный подход представляется вполне оправданным как наиболее простой и практически применимый.

Используя синтезирующий подход к формированию авторской позиции по рассматриваемому вопросу, предлагаем следующую классификацию цифровых следов:

I. По видам преступной деятельности следует различать:

1. Следы преступлений, предусмотренных главой 31 Уголовного кодекса Республики Беларусь «Преступления против компьютерной безопасности».

2. Следы преступлений, совершенных с использованием сети Интернет (доведение до самоубийства, развратные действия, мошенничество, азартные игры, сбыт наркотических средств и т. д.).

3. Следы иных преступных деяний (совершенных в том числе по неосторожности).

II. В зависимости от места обнаружения:

1. Следы, обнаруженные в мобильных цифровых устройствах (смартфоны, электронные книжки, часы, флеш-накопители, карты памяти, фитнес-браслеты, пульсометры, шагомеры и пр.).

2. Следы, обнаруженные в стационарных устройствах (компьютеры, моноблоки, серверы, автомобильные регистраторы, бортовые самописцы, авторегистраторы, системы безопасности и пр.).

3. Следы, обнаруженные в приборах смешанного типа (видео-, фотоаппаратура, ноутбуки, квадрокоптеры и др.).

III. В зависимости от решаемых конечных и промежуточных целей органа дознания и предварительного следствия:

1. Следы, позволяющие проверить местонахождение участника досудебного производства (а точнее, принадлежащего ему устройства) [9, с. 112], метаданные

фотографий, видеовкладки, привязку технического устройства (смартфона, планшета) к Wi-Fi-роутерам, а также данные программных приложений, сохраняющие криминалистически значимую информацию (службы такси, каршеринга и пр.).

2. Следы, позволяющие получить информацию о готовящемся, совершаемом или скрываемом преступлении, его соучастниках, жертвах, новых эпизодах (СМС, голосовые сообщения, фото, переписка в чатах, социальных сетях, история браузера пользователя, данные записной книжки).

IV. По значимости для процесса выявления, раскрытия и расследования преступления цифровые следы можно разделить на:

1. Непосредственно уличающие лицо в совершении преступления (фотоизображения, видеозаписи в момент его совершения, переписка, явно либо косвенно указывающая на причастность к противоправному деянию).

2. Ориентирующие и направляющие ход расследования (точка последнего соединения; установление свидетеля; информация, опровергающая, устанавливающая либо дополняющая какие-либо факты или события).

Разработанная классификация может быть дополнена и иными основаниями, которые имеют как теоретическое, так и прикладное значение, например, процессами формирования и движения цифровых следов.

Изложенное позволяет сделать следующие выводы:

1. Анализ литературы по вопросам исследования цифровых следов в криминалистической науке позволяет сделать вывод о том, что в настоящее время отсутствует доминирующая позиция определения сущности цифровых следов, подходов к формулировке основных понятий, терминов и их определений.

2. Многоаспектность исследуемой проблемы делает затруднительным выработку единообразного подхода к построению классификации цифровых следов. Указанное обстоятельство обусловлено множеством оснований в предложенных исследователями авторских классификациях.

3. Электронно-цифровые следы представляют собой цифровой код, возникающий в процессе преобразования первичных электронных сигналов в электронном устройстве, характеризующийся пространственно-временными параметрами, фиксирующийся и отражающийся в преобразованной (воспринимаемой) форме на материальном носителе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Философский словарь : в 5 т. / под ред. Ф. В. Константинова. — М. : Сов. энцикл., 1960. — Т. 4 — 592 с.

2. Философский словарь / под ред. М. М. Розенталя. — 3-е изд. — М. : Политиздат, 1975. — 496 с.

3. Белкин, Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории / Р. С. Белкин. — М. : Юрид. лит., 1987. — 272 с.

4. Осипенко, А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс / А. Л. Осипенко // Науч. вестн. Ом. акад. МВД России. — № 4(35). — 2009. — С. 20–25.

5. Колычева, А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. ... канд. юрид. наук : 12.00.12 / А. Н. Колычева. — М., 2019. — 200 с.

6. Барченкова, Я. В. Цифровые следы при расследовании мошенничества, совершенного при помощи средств сотовой связи / Я. В. Барченкова // Современная наука: актуальные проблемы теории и практики. — № 4. — 2020. — С. 135–138.

7. Себякин, А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации : дис. ... канд. юрид. наук : 12.00.12 / А. Г. Себякин. — М., 2021. — 271 с.

8. Жижилева, А. А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы [Электронный ресурс] / А. А. Жижилева // Вопросы российской юстиции. — 2019. — № 3. — Режим доступа: https://cyberleninka.ru/article/n/o-nekotoryh-teoreticheskih-aspektah-ispolzovaniya-v-kriminalistike-ponyatiy-tsifrovye-elektronnye-virtualnye-sledy. —Дата доступа: 10.05.2022.

9. Васюков, В. Ф. Теоретические и правовые аспекты расследования преступлений с использованием абонентской информации : монография / В. Ф. Васюков ; под ред. д-ра юрид. наук А. Г. Волеводза. — Орел : Картуш, 2020. — 339 с.

Поступила в редакцию 13.05.2022 г.
Контакты: ord@institutemvd.by (Апекунов Александр Сергеевич),
k99nastya.kowaltschuk@gmail.com (Варванович Анастасия Сергеевна)

Apekunov A. S., Varvanovich A. S.
TO THE QUESTION OF THE CLASSIFICATION OF DIGITAL TRAILS

The article considers theoretical approaches to the construction of a classification of digital traces in forensic science. It has been determined that at present there is no dominant position in forensic science to define the essence of digital traces. Based on the analysis of existing scientific views on the designated problem, the author's classification is proposed, the essence of digital traces is determined from the point of view of the nature of their occurrence and existence.

Keywords: *electronic footprint, virtual footprint, information footprint, digital footprint, digital footprint, cybercrime.*